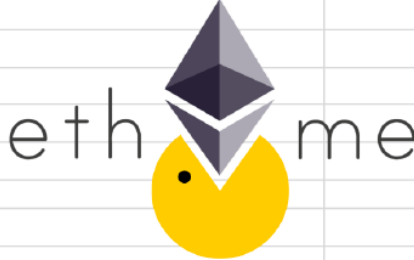


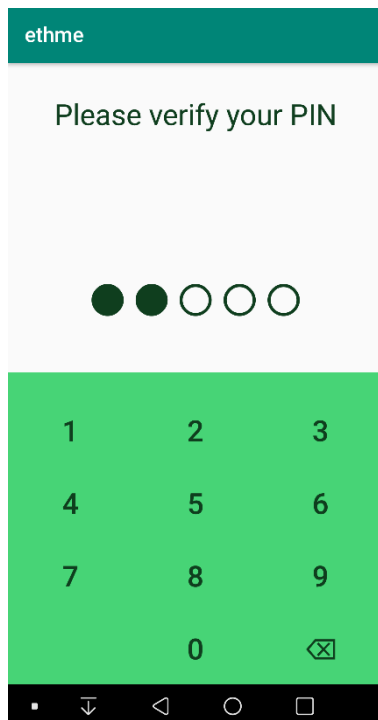
ETHME – Status Update II

ETHME time & task recording				
project workload	125,00 h		team size	1 persons
per person	125,00 h			
workload left over	77,00 h		start	23.9.2019
per person	77,00 h		end	14.10.2019
			duration	3 weeks
left h per week / person	59,89 h		today	05.10.2019
per working day	9,98 h		till end	1 weeks
Projects GitHub:	https://github.com/arminbrandy/ethme		total	48,00 h
Armin Brandy				
task - *commit			hours	date
Research & evaluation			4,00 h	23.09.2019
Defining and writing the Vision as "Whitepaper" - look at init commit - *ebbcc22			2,00 h	23.09.2019
Start reading Mastering Ethereum			3,00 h	26.09.2019
Setup Project, basic environment & GitHub			3,00 h	27.09.2019
FH Blockchain LV - more about blockchain			3,00 h	27.09.2019
Starting Project, more environment & creating basic App - *4b636ea			4,00 h	28.09.2019
ETHME - Status Update I			1,25 h	28.09.2019
Working on connecting to node via web3j and on Wallet creation...			4,50 h	29.09.2019
Successfully testing first web3j Wallet functionalities with web3j doc			4,50 h	02.10.2019
Learning about Wallet standards as BIP39/44 and related, Javas 'true' SecureRandom fns Exploring & testing wallet creation & storage with web3j and understanding the concepts			7,50 h	03.10.2019
Concept of user auth to access wallet & PIN activity for user authentication			2,75 h	04.10.2019
FH Blockchain LV - more into Ethereum & smart contracts			3,25 h	04.10.2019
Design PIN activity & designing secure storage structure			4,00 h	05.10.2019
ETHME - Status Update II			1,25 h	05.10.2019

Progress

This week was very theory loaded. A lot of researching was done about topics like, how the web3j library works, how wallets are created & stored, about the standards BIP-39 & BIP-44/32, how random SecureRandom numbers from java really are and also about Android, its KeyStore functionality and it's developing in general, since this also is a new area with this project.

The motivation behind these researches are, to understand what's actually happening by using the web3j functions and working with walletfiles. In order to be capable of better estimating the security risks and the security management which comes with working with these technologies. Therefore, being able to implement the App as secure as possible, in the scope of this project.



Along with the research a lot of try out of the web3j Wallet functionalities was done and also first test walletfiles were created (see Screenshot below).

Also, a PIN input activity was built and nicely designed.

You could say, a lot of different tools and functionalities have been explored, learned and prepared to put all that know how together in the following steps.

Since that was quite a steep learning curve so far, there's no working wallet functionality and therefore no useful code to push yet. But as far as the project can be seen right now, it seems that the wallet management will be a bigger part of that project compared to other tasks for the mvp version.

The basic idea for the wallet management is, to store it as secure as possible. Ideally using Androids own KeyStore functionality to encrypt it and restrict its access only to the App itself in combination with user authentication.

```

1  {
2  "address": "c63aa1000395d5ffe685438a409a6da4a9fbf7b8",
3  "id": "7ecd72c-7541-4a3f-b37e-fff427663799",
4  "version": 3,
5  "crypto":
6  {
7    "cipher": "aes-128-ctr",
8    "cipherparams":
9    {
10     "iv": "f16522ce002820810125b7191ab225e9"},
11    "ciphertext": "8ea7268b66b23d58c838679bfc6364381bd7a56cd1bfff71f4b3a4343d5b4153f",
12    "kdf": "scrypt",
13    "kdfparams":
14    {
15     "dklen": 32,
16     "n": 4096,
17     "p": 6,
18     "r": 8,
19     "salt": "a4ddf2cc7ca7d740d82277a7256fdb0b3c2a051d3b358a6d327452357b82f8ad"},
20     "mac": "0bd52fbc6417919925525fe79ea3da5483b9ac299736d87c7d867f72d2ba1de"}
21   }
22 }

```

How are we proceeding

Regarding the development ...

As planned - implementing the whole wallet management which will consist of:

- Creating, requesting and changing User Authentication (PIN and maybe later fingerprint) in combination with Android KeyStore.
- Creating the wallet and check that the user also wrote down its mnemonic seed.
- Using both above steps to actually store the wallet file securely encrypted.
- At last step, of course to also make the wallet available, if it's needed to sign a TX, using above functionalities.

After the wallet management, receiving and sending ETH shall be easily possible.

Regarding the management ...

The project is in a good process and seems to develop in a good direction.

Only challenge, as already suspected beforehand, would be the time management. Which probably won't be enough to fulfil all the 125h of workload, defined by the 5 ECTS.

However, the App in it's mvp version, as described in the Whitepaper, still seems to be plausible to implement in the timeframe before deadline, the 14th Oct.

In following cases I'd suggest slightly adjustments to the project conditions:

- If the mvp version is finished, but there's still workload left. The Design of the App can be improved and extra features could be implemented.
- If the deadline of the 14th Oct. should not be enough time to finish the mvp, but the project has noticeable progress in development, I'd suggest an adjustment to at least Friday the 18th Oct. or if that would also make sense to Sunday the 20th Oct.

I'd like to decide these questions latest by the next Status Update nr. 3 on Friday 11th Oct.